

Messenger-Dienste

Kommunikation unter eigener Kontrolle

[10.09.2026] Digitale Souveränität entscheidet sich auch bei der täglichen Kommunikation. Kommunen sollten deshalb darauf achten, wer Zugriffe kontrolliert, wie transparent die eingesetzte Software ist und ob Kommunikationswege auch im Krisenfall funktionieren. Eine Alternative zu US-amerikanischen Messenger-Diensten bietet Threema.

E-Mail, Messenger und Kollaborationsplattformen gehören längst zur Grundausstattung einer Verwaltung. Über sie werden täglich sensible Informationen ausgetauscht, Entscheidungen vorbereitet und Arbeitsabläufe koordiniert. Damit wird die Kommunikation zu einem wichtigen Baustein digitaler Souveränität. Kommunen müssen entscheiden können, wie ihre Daten verarbeitet werden, wer darauf zugreifen kann und welche Alternativen bei einem Ausfall zur Verfügung stehen.

Eine Rolle spielt dabei die Transparenz der eingesetzten Software. Quelloffene Anwendungen bieten die Möglichkeit, sicherheitsrelevante Funktionen unabhängig zu überprüfen. „Ein offener Quellcode wie beispielsweise bei unserem Business-Messenger Threema Work schafft volle Transparenz und erlaubt externen Fachpersonen, wesentliche Funktionen der Anwendung, wie die Umsetzung der Verschlüsselung oder den Umgang mit Schlüsseln, einzusehen und unabhängig zu untersuchen“, erläutert Danilo Barga, CTO bei [Threema](#). Quelloffenheit allein sei allerdings noch kein Qualitätsmerkmal. Entscheidend sei ebenso, ob der Code gepflegt, regelmäßig überprüft und aktualisiert werde.

Abhängigkeiten reduzieren

Eng damit verbunden ist die Frage, wie stark sich eine Kommune an einen einzelnen Anbieter bindet. Offene und dokumentierte Schnittstellen können dazu beitragen, einen Vendor-Lock-in zu vermeiden und Kommunikationsdienste in bestehende IT-Landschaften einzubinden. Threema bietet dafür beispielsweise einen Gateway-Service an, mit dem Nachrichten auf der eigenen Infrastruktur verschlüsselt, versendet, empfangen und entschlüsselt werden können.

Zur digitalen Souveränität gehört auch die Wahl des Betriebsmodells. Cloud-Dienste sind schnell verfügbar, skalierbar und können die kommunale IT bei Wartung und Aktualisierung entlasten. Gerade bei begrenzten Ressourcen kann Software as a Service (SaaS) deshalb sinnvoll sein. Geprüft werden sollte allerdings, wo der Anbieter seinen Sitz hat, welcher Gerichtsbarkeit er unterliegt und wie er mit Daten und Metadaten umgeht. Threema verweist in diesem Zusammenhang auf seinen Sitz in der Schweiz und darauf, nicht dem US CLOUD Act zu unterliegen. Die Datenverarbeitung erfolgt nach Angaben des Unternehmens in ISO-27001-zertifizierten Rechenzentren in der Schweiz.

Für Verwaltungen mit besonders hohen Anforderungen kann eine selbst betriebene On-Premises-Lösung eine Alternative sein. Damit geht allerdings zusätzliche Verantwortung einher. Die Kommune muss unter anderem Updates, Monitoring, Back-ups und Verfügbarkeit selbst sicherstellen. „Eine On-Premises-Lösung ist jedoch nicht in allen Fällen automatisch sicherer“, sagt Barga. Digitale Souveränität bedeutet deshalb nicht zwangsläufig Eigenbetrieb, sondern auch die Möglichkeit, je nach Schutzbedarf und Ressourcen zwischen verschiedenen Betriebsformen zu wählen.

Kommunikation im Krisenfall

Wie wichtig technologische Unabhängigkeit ist, zeigt sich besonders in Krisensituationen. Fällt die zentrale E-Mail- oder Kollaborationsplattform infolge einer Störung oder eines Cyber-Angriffs aus, braucht die Verwaltung einen vorbereiteten Ausweichkanal. Darüber sollten sich beispielsweise die gesamte Belegschaft, einzelne Organisationseinheiten oder externe Partner kurzfristig erreichen lassen.

Ein Business-Messenger kann einen solchen Backup-Kanal bereitstellen. Voraussetzung ist, dass er bereits vor einem Vorfall eingerichtet und in die Notfallplanung integriert wurde. Beschäftigte sollten den Kommunikationsweg kennen und möglichst schon im Arbeitsalltag nutzen. „Digitale Souveränität in der Kommunikation bedeutet, dass Verantwortliche auch dann Informationen sicher und zuverlässig austauschen und Entscheidungen koordinieren können, wenn etablierte Kommunikationswege beeinträchtigt sind“, fasst Barga zusammen. Die Abhängigkeit von nur einem Kommunikationskanal erhöht dagegen die Verwundbarkeit.

Inhalte und Metadaten schützen

Ein weiterer Baustein ist die Verschlüsselung. Bei einer konsequenten Ende-zu-Ende-Verschlüsselung können Nachrichteninhalte nur von Sender und Empfänger gelesen werden. Auch der Betreiber des Dienstes erhält keinen Zugriff darauf. Mindestens ebenso relevant ist der Umgang mit Metadaten. Schon die Information, wer wann mit wem kommuniziert, kann Rückschlüsse auf Personen, Zuständigkeiten und interne Vorgänge erlauben. Kommunikationslösungen sollten deshalb möglichst nur jene Daten verarbeiten, die für ihren Betrieb tatsächlich erforderlich sind.

Souveränität betrifft darüber hinaus die Nutzer- und Rechteverwaltung. Eine Organisation sollte selbst bestimmen können, wer auf welche Kommunikationsräume und Informationen zugreifen darf. Dafür sollte sich ein dienstlicher Messenger zentral administrieren und möglichst an vorhandene Verzeichnisdienste anbinden lassen. Nutzer können dann automatisiert eingerichtet, Rollen vergeben und Konten beim Ausscheiden aus der Verwaltung deaktiviert werden.

Bei Threema Work sind dafür unter anderem die Einbindung in ein Mobile Device Management und die Administration über ein zentrales Management-Cockpit vorgesehen. Funktionen zur Kontaktverifizierung und zur Beschränkung auf interne Kontakte sollen zusätzlich verhindern, dass Unbefugte Zugang zu dienstlichen Informationen erhalten.

()

Stichwörter: Digitale Souveränität, Messenger, Threema